CLAIMS

1   1.   A distributed network having a plurality of processors, the network
2   hardware and software comprising:
3   a local counter associated with each of the processors in the distributed
4   network;
5   an event register associated with each of the local counters; and
6   an event logger for receiving a counter value from the local counter in response
7   to an event being registered in the event register.

1   2. The distributed network of claim 1 comprising a global clock wherein a
2   time stamp is calculated based on the counter value received from a counter associated
3   with a processor in the distributed network.

1   3. The distributed network of claim 1 wherein the event logger records data
2   concerning a type of event registered by the event register and a time an event
3   occurred.

1   4. The distributed network of claim 1 wherein the event register remains
2   frozen until the event register is read by the system monitor.

1   5.   The distributed network of claim 1 comprising dynamic masking
2   mechanisms for filtering the event register outputs to differentiate between critical and
3   non-critical events.

1   6. The network of claim 5 wherein the masking is dynamically updated during
2   online processing.

1   7. The network of claim 1 comprising software for performing conditional
2 probability calculations based on event information stored in a history table wherein
3 the calculations are performed to determine if a probability of an event occurring has
4 exceeded a minimum threshold level and, if the threshold is exceeded, to migrate a
5 process or schedule maintenance to avoid consequences of the predicted event.

1   8. The network of claim 7 wherein the conditional probability calculations are
2 based upon events occurring within a selected time window.

1   9. The network of claim 1 wherein the event register comprises an error time
2 stamp register that receives a value from the local counter when an event occurs.

1   10. The network of claim 1 wherein the event register stores an error occurred
2 value that indicates to the network monitor that a critical event has occurred.

M

1   11. A method of producing a time stamp for an event occurring on a
2   distributed network including a plurality of processors comprising:

3   producing a local counter value for each of a plurality of processors in the
4   distributed network with an associated counter;

5   synchronizing the local counter at each of the processors with a global clock;
6   and

7   freezing the local counter for a processor when a critical event associated with
8   the processor occurs.

1   12. The method of claim 11 comprising establishing a history table containing
2   information concerning events associated with the critical event and the conditional
3   probabilities of the associated events during offline processing.

1   13. The method of claim 12 comprising determining during an offline phase if
2   an event is critical and whether or not online processing is possible.

1   14. The method of claim 12 comprising dynamically filtering the events based
2   on a recorded history of information associated with the occurrence of events such that
3   only certain critical events produce global interrupts.

1   15. The method of claim 12 comprising updating the conditional probability
2   information and history table during offline processing.

1   16. The method of claim 11 comprising determining during online processing

2   a type of event that occurred and determining whether to produce a global alert, synch

3   stop or machine check alert signal based upon the type of event that occurred.

1   17. The method of claim 11 comprising dynamically masking events that

2   occur based on conditional probabilistic calculations using machine learning

3   algorithms to predict an occurrence of a critical event during a specified time period.

1   18. A distributed computer system having hardware and software for

2   implementing a time stamping process for producing a time stamp associated with an

3   occurrence of an error event, the computer system comprising:

4   a plurality of local counters wherein each counter is associated with a

5   particular processor or system in the distributed computer system;

6   an event register for recording event information concerning an occurrence of

7   an event associated with the processor and event register; and

8   an event logger for receiving and logging information concerning the

9   occurrence of the events.

1   19. The distributed computer system of claim 18 comprising a global clock for

2   synchronizing the local counters.

1   20. The distributed computer system of claim 19 wherein the event logger

2   records a time stamp based upon the global clock and a local counter value received

3   from a local counter.

1   21. The distributed computer system of claim 18 comprising dynamic masks

2   created based upon historical event information for filtering events such that only

3   information concerning critical events result is stored.

1   22. The distributed computer system of claim 21 comprising software for

2   evaluating events based on conditional probabilistic calculations and scheduling

3   remedial or preventative action during online processing.

1   23.   A computer-executable medium comprising instructions for producing

2   a time stamp for an event occurring on a distributed network including a plurality of

3   processors, the medium comprising instructions for:

4   producing a local counter value for each of a plurality of processors in the

5   distributed network with an associated counter;

6   synchronizing the local counter at each of the processors with a global clock;

7   and

8   freezing the local counter for a processor when an event associated with the

9   processor occurs.

1   24.   The medium of claim 23 comprising an instruction for monitoring the

2   local counter with a system monitor through the use of online and offline processing.

1   25.   The medium of claim 23 comprising an instruction for periodically polling

2   the local counters and storing information received in a history table.

1   26.   The medium of claim 23 comprising an instruction for dynamically

2   filtering the events based on a recorded history of information associated with the

3   occurrence of events such that only critical events are reported to a system monitor.

1   27.   The medium of claim 23 comprising an instruction for performing

2   conditional probability calculations to determine if a probability that a critical event

3   will occur exceeds a threshold level and performing or scheduling preventative action

4   if such threshold is exceeded.

1   28. The medium of claim 11 comprising an instruction for determining a type

2 of event that occurred and determining whether to produce a global alert, synch stop or

3 machine check alert signal based upon the type of event that occurred.

1   29. The medium of claim 11 comprising an instruction for dynamically

2 masking events that occur based on conditional probabilistic calculations using

3 machine learning algorithms.